

Achtung, DB-Kunden! Phishing-Warnung: So schützen Sie Ihre Daten!

Verbraucherzentrale warnt vor Phishing-Attacken auf Deutsche-Bahn-Kunden. Erfahren Sie, wie Sie sich schützen können.



Verbraucherzentrale NRW, Deutschland - Die Verbraucherzentrale warnt vor einer aktuellen **Phishing-Attacke**, die gezielt Kunden der Deutschen Bahn (DB) ins Visier nimmt. In den vergangenen Tagen haben zahlreiche Nutzer E-Mails mit dem Betreff „Ihr Konto erfordert eine Aktualisierung“ erhalten. Darin wird behauptet, es seien „verdächtige Aktivitäten“ auf ihren Konten festgestellt worden.

Die Betrüger, die hinter diesen Mails stecken, fordern die Empfänger dazu auf, ihre Identität zu verifizieren. Dazu wird angegeben, dass eine „Verifizierung mittels einer gültigen Kreditkarte“ notwendig sei. Der Druck wird durch eine kurze Reaktionsfrist von lediglich 12 Stunden erhöht, innerhalb derer

die Kunden handeln sollen, um mögliche Zugangsbeschränkungen zu vermeiden. Zudem wird in den E-Mails behauptet, dass ein Euro abgebucht werde, der jedoch nach der Überprüfung zurückerstattet wird.

Typische Phishing-Merkmale

Die Warnungen der Verbraucherzentrale basieren auf typischen Phishing-Merkmalen, die in den E-Mails zu erkennen sind. Diese umfassen:

- Unpersönliche Anrede
- Kurze Fristsetzung von 12 Stunden
- Drohung mit Zugangsbeschränkungen
- Aufforderung zur Kreditkartenverifizierung

Um sich vor diesen Angriffen zu schützen, empfehlen die Experten, solche E-Mails zu ignorieren und sie in den Spam-Ordner zu verschieben. Offizielle Informationen zu Verifizierungsmaßnahmen sollten ausschließlich über die offizielle DB-Website oder die Bahn-App eingeholt werden, da seriöse Unternehmen niemals per E-Mail zur Eingabe sensibler Daten auffordern.

Vorsicht bei Verdacht auf Betrug

Die Verbraucherzentrale rät den Betroffenen, bei Verdacht auf Betrug folgende Schritte zu unternehmen:

- Die Bank kontaktieren und die Kreditkarte sperren lassen.
- Passwörter zum DB-Konto sowie ähnliche Zugangsdaten ändern.
- Den Vorfall bei der Polizei melden.

Phishing-Attacken sind nicht nur eine Bedrohung für die finanziellen Daten der Kunden, sondern auch für deren persönliche Informationen. Betrüger versuchen, Passwörter und

Kreditkarteninformationen zu erlangen, häufig durch gefälschte E-Mails oder Websites, die echt aussehen. Die **Deutsche Bahn** weist zudem darauf hin, dass Verbraucherzentralen ein „Phishing-Radar“ anbieten, um über aktuelle betrügerische Aktivitäten zu informieren.

Die Folgen von Identitätsdiebstahl

Wird es Kriminellen gelungen, persönliche Daten der Opfer zu erlangen, können die Folgen gravierend sein. Laut der **Verbraucherzentralen** wird Identitätsdiebstahl häufig genutzt, um im Namen der Opfer kostenpflichtige Abonnements, Nutzerkonten oder Waren im Internet abzuschließen. Geschädigte erfahren oft erst durch Rechnungen oder Inkassoschreiben von einem möglichen Identitätsmissbrauch.

Zu den häufigsten Fällen zählen unberechtigt abgeschlossene Abonnements für Streaming-Dienste oder Online-Services sowie unautorisierte Warenbestellungen. In diesem Zusammenhang können persönliche Informationen wie Name, Geburtsdatum und Kontoinformationen für weiteren Identitätsmissbrauch verwendet werden, was die Wichtigkeit von schnellem Handeln im Verdachtsfall unterstreicht.

Um sich und seine Daten zu schützen, sollten Verbraucher starke Passwörter verwenden und verdächtige E-Mails sofort löschen. Bei Verdacht auf einen Identitätsdiebstahl ist es entscheidend, schnell zu handeln, die Bank zu informieren und gegebenenfalls eine Strafanzeige zu stellen.

Details	
Vorfall	Phishing
Ort	Verbraucherzentrale NRW, Deutschland
Schaden in €	900
Quellen	<ul style="list-style-type: none">• www.ruhr24.de• www.bahn.de• www.verbraucherzentrale.de

Besuchen Sie uns auf: n-ag.de